SIDLEY

Switzerland Recognizes New EU Standard Contractual Clauses and Issues Guidance on International Data Transfers

Sabrine Schnyder

On August 27, 2021, the Swiss Federal Data Protection and Information Commissioner (FDPIC) formally recognized the new EU Standard Contractual Clauses published by the European Commission on June 4, 2021 (New SCCs). The New SCCs are intended to legitimize transfers of personal data from Switzerland to countries not deemed by the FDPIC as providing an adequate level of protection for personal data (cf. official statement). By recognizing the New SCCs and thereby completing its guidance on international data transfers published on June 18, 2021, the FDPIC reduces uncertainties in a post-Schrems II era and helps companies ensure the ongoing lawful transfer of personal data.

As of September 27, the use of the New SCCs in new and substantially amended contracts is mandatory and companies are required to conduct detailed transfer risk assessments. Hence, companies should take immediate steps to ensure compliance with these requirements.

A. General Principles Applicable to International Data Transfers

As a reminder, the Federal Act on Data Protection (FADP) prohibits the transfer of personal data from Switzerland to a third country that has not been deemed to provide an adequate level of protection by the FDPIC (Article 6(1) FADP) — for example, the U.S. The FDPIC has published an indicative list of countries that it considers have adequate data protection laws. However, the ultimate responsibility for determining adequacy lies with the data exporter. In turn, when seeking to rely on the list, a data exporter must check periodically whether the protection is still adequate and whether there are any reasons to believe that this is no longer the case (e.g., practical experience or reports in the media). This said, the FDPIC's guidance is silent on whether the exporter has an *active* obligation to monitor the legal situation in the destination country.

B. The New SCCs

Where a third country is not considered adequate, the data exporter should identify a data transfer mechanism to legitimize the transfer of personal data. One such mechanism is the New SCCs. The New SCCs (published by the European Commission in June 2021) take into account the Court of Justice of the EU's decision in *Schrems II*, and requirements under the EU General Data Protection Regulation (GDPR). As compared to the former standard contractual clauses (Old SCCs), the New SCCs are significantly more onerous in terms of the number and scope of obligations as well as considerably longer. However, their formulation (i.e., the multiple transfer scenarios addressed — including transfers from processors) greatly facilitates the "widespread use of new and more complex processing operations."

When looking to implement the New SCCs, a company should as a first step, identify the appropriate module that applies to the specific transfer:

- Module 1: controller to controller
- Module 2: controller to processor
- Module 3: processor to (sub)processor
- Module 4: processor to controller

In a second step, the exporter will have to adapt the New SCCs to reflect Swiss law, for example, replace references to the GDPR with references to the FADP, include reference to the FDPIC as the competent supervisory authority, and, until entry into force of the revised FADP, extend the scope of application to include personal data of legal entities. This can be done via, for example, an addendum to the New SCCs.

In terms of timing, for Switzerland (1) the New SCCs must be used as of **September 27, 2021,** for any new data transfers (or data transfers that have substantially changed); and (2) existing agreements relying on the Old SCCs must be replaced with the New SCCs by **January 1, 2023**.

Finally, the Swiss organization must inform the FDPIC of its proposed use of the New SCCs (Article 6(3) FADP and Article 6 Ordinance to the FADP), although this obligation ceases to exist with the entry into force of the revised FADP, expected in late 2022/early 2023.

C. Requirement to Conduct a Foreign Law Assessment

When using the New SCCs (or another contractual safeguard pursuant to Article 6(2)(a) FADP), an organization must conduct a detailed assessment of its international data transfers. This means that the data exporter should:

(1) keep a detailed record of the international data transfers, for example, categories of personal data, data subjects involved, the length of the processing chain (processors, subprocessors, etc.), the purpose of the data transfer, the means of transfer (e.g., email or remote), the format of the personal data transferred (e.g., encrypted/pseudonymized), and the economic sector in which the transfer occurs

(2) evaluate whether access to personal data by public authorities and data subject rights in the third country are in line with the following Swiss fundamental rights:

- *Principle of legality:* The legal system of the third country should have specific and clear legal provisions limiting access to personal data by public authorities.

- *Proportionality of the powers and measures of public authorities:* The powers and measures available to the authorities must be suitable and necessary for the authorities to fulfill the legal purposes of their access. In addition, they must be reasonable as far as the data subjects are concerned.

- *Remedies:* Data subjects must be vested with effective legal remedies to enforce their rights such as rights of access, rectification, and deletion.

- *Judicial system:* The legal system of the third country should provide for a guarantee of legal recourse and access to an independent and impartial court.

When carrying out this evaluation, the exporter should take into account applicable legislation, practices of administrative and judicial authorities, and case law. The FDPIC makes clear that subjective factors, such as the likelihood of access, should not be considered. To help exporters with their evaluation, the FDPIC has published a questionnaire to be used for transfers to the United States.

If it is determined that practices in the third country align with the Swiss fundamental rights, reliance on the New SCCs (and indeed the Old SCCs) should in principle be sufficient. Otherwise, the exporter must put in place additional contractual, technical, and organizational measures to address any perceived gaps in the third country. Such supplementary measures may include, for example, confidentiality obligations imposed on the importer, protective orders, encryption prior to transfer or remote-only access to personal data saved on an EU or Swiss server. If this is not possible, the transfer is not permitted.

D. Alternatives to the New SCCs

The New SCCs are not the only legal transfer mechanism, and a data exporter can explore other options such as binding corporate rules for international intragroup transfers or other individually negotiated data transfer agreements. Also, the FDPIC has announced that it will publish an updated version of the Swiss Transborder Data Flow Agreement at a later stage, providing an additional option to data exporters. However, the requirements for these alternatives are often more burdensome (e.g., approval by FDPIC). In certain limited cases, the exporter may alternatively rely on the derogations listed in Article 6(2) FADP, such as the legal defense exemption, performance of a contract, or consent of the concerned data subject.

E. Next Steps

Companies will need to carefully consider the New SCCs to determine which of the modules applies to their data transfer scenarios, add an addendum for their use in Switzerland, and determine how they and other parties will comply with contractual obligations in the New SCCs. Furthermore they should plan how to best roll out the New SCCs both for intragroup transfers but also data transfers to third parties. Companies will also need to ensure they have carried out a *Schrems II* data transfer assessment project and considered the use of the New SCCs in this context.